means for verifying the validity of the access token based on a comparison of the authentication password to the security policy;

means for setting security policies in the computer system; and

means for unlocking a nonvolatile storage device on the computer system.

B1 cont

42. **(Twice Amended)** An information handling system comprising:

means for reading an access token containing a security policy for the information handling system;

means for receiving an authentication password from a user;

means for verifying the validity of the access token based on a comparison of the authentication password to the security policy;

means for setting security policies in the information handling system; and

means for unlocking a nonvolatile storage device on the information handling system.

REMARKS

Applicants have carefully reviewed this application in light of the Final Office Action mailed October 23, 2002. Claims 1-38 and 40-42 are pending in this application. Claims 1-5, 9-14, 16-25, and 35-38, 40-42 are rejected. Claims 6-8 and 26-34 are allowed and Claim 15 is objected to as being dependent upon a rejected claim. Applicants previously cancelled Claim 39 without prejudice or disclaimer. Applicants have amended Claims 1, 2, 8, 15-25, 35, and 40-42 to further define that which Applicants regard as their invention and respectfully request reconsideration and favorable action in this case.

Rejections under 35 U.S.C. § 101

Claim 40 stands rejected by the Examiner under 35 U.S.C. § 101 as not constituting statutory subject matter. Applicants respectfully traverse and submit that amended Claim 40 is patentable. Applicants respectfully request reconsideration and withdrawal of the rejection and allowance of amended Claim 40.

Objected Claims

Claim 15 is objected to by the Examiner as being dependent on a rejected base claim. Applicants have amended Claim 15 to include the limitations of the base claim. Applicants request withdrawal of the objection and allowance of amended Claim 15.

Rejections under 35 U.S.C. § 103

Claims 1-5, 9-14, 16-25, 35-38, 40-42 stand rejected by the Examiner under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,949,882 issued to Michael F. Angelo (hereinafter "Angelo") and Authoritative Dictionary of IEEE Standards (hereinafter "IEEE Standards") in view of U.S. Patent No. 6,282,649 issued to Howard Shelton Lambert (hereinafter "Lambert"). Applicants have Claim 14 without prejudice or disclaimer. Applicants respectfully traverse and submit that Claims 1-5, 9-13, 16-25, 35-38, and 40-42, as amended, are patentable over Angelo and IEEE Standards in view of Lambert.

Angelo discloses a two piece authentication procedure to enable access to secured computer resources (col. 3, lines 30-31). The procedure uses a token or smart card "to store an encryption algorithm furnished with an encryption key that is unique or of limited production" (col. 3 lines 37-39). The encryption algorithm is used to encrypt a user-entered password to create a "peripheral" password to permit access to the secured resource (col. 3, lines 41-48).

Lambert discloses an access control system that utilizes hierarchical user keys, which have different access keys for different access levels.

Applicants' amended Claim 1 calls for various features including "an executable program code that verifies validity of the access token by comparing the security code to a verification data on the access token, whereby if the security code matches verification data the access token is valid."

Applicants' amended Claim 35 recites, in part, "matching a computer system password with the user input password with the one or more passwords from the access token to access the computer system, wherein the computer system password includes one or more security policies configured in the computer system."

Applicants' amended Claim 40 calls for various features including "a security code stored on the access token, wherein the communication device transmits the one or more security policies in response to receiving an authentication code corresponding to the security code."

Applicants' amended Claim 41 calls for various features including "means for reading an access token containing a security policy for the computer system," and "means for

verifying the validity of the access token based on a comparison of the authentication password to the security policy."

Applicants' amended Claim 42 calls for various features including "means for reading an access token containing a security policy for the information handling system," and "means for verifying the validity of the access token based on a comparison of the authentication password to the security policy."

Neither Angelo, IEEE Standards, nor Lambert make obvious Claims 1-5, 9-13, 35-38 and 40-42, as amended, of Applicants' invention because Angelo, IEEE Standards, or Lambert fails to teach disclose, or suggest all of the elements recited in Claims 1-5, 9-13, 35-38 and 40-42, as amended. For example, the cited references fail to disclose "an executable program code that verifies validity of the access token by comparing the security code to a verification data on the access token, whereby if the security code matches verification data the access token is valid" as recited in amended Claim 1. As further recited in amended Claim 35, Angelo, IEEE Standards, or Lambert fails to disclose, suggest, or teach "matching a computer system password with the user input password with the one or more passwords from the access token to access the computer system, wherein the computer system password includes one or more security policies configured in the computer system."

As further recited in amended Claim 40, Angelo, IEEE Standards, or Lambert fails to disclose, suggest, or teach "a security code stored on the access token, wherein the communication device transmits the one or more security policies in response to receiving an authentication code corresponding to the security code." As recited in amended Claim 41, Angelo, IEEE Standards, or Lambert fails to disclose, suggest, or teach "means for reading an access token containing a security policy for the computer system," and "means for verifying the validity of the access token based on a comparison of the authentication password to the security policy." As recited in amended Claim 42, Angelo, IEEE Standards, or Lambert fails to disclose, suggest, or teach "means for reading an access token containing a security policy for the information handling system," and "means for verifying the validity of the access token based on a comparison of the authentication password to the security policy." Applicants therefore respectfully request the Examiner to reconsider and withdraw the rejection to and allow amended Claims 1, 35 and 40-42.

Claims 2-5 and 9-13, as amended, directly or indirectly depend from and provide further patentable limitations to amended Claim 1. Amended Claims 16-25 directly or indirectly depend from and provide further patentable limitations to Claim 15. Claims 36-38 directly or indirectly depend from and provide further patentable limitations to Claim 35. Because Claims 6, 15, and 35, as amended, are deemed allowable, Claims 2-5, 9-13, 16-25, and 36-38, as amended, are allowable. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw the rejection to and allow Claims 1-5, 9-13, 16-25, 35-38, and 40-42, as amended.

Allowable Subject Matter

Applicants appreciate the Examiner's careful review of the application and allowance of Claims 6-8 and 26-34.

CONCLUSION

Applicants have now made an earnest effort to place this case in condition for allowance in light of the amendments and remarks set forth above. Applicants respectfully request reconsideration of the rejections and allowance of the claims, as amended.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendments. The attached pages are captioned "**Version with Markings to Show Changes Made.**"

Applicants believe no fee is due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0383 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants

Patrick J. Porter
Reg. No. 45,658

Date: December 23, 2002

Correspondence Address:
One Shell Plaza
910 Louisiana
Houston, Texas 77002-4992
512.322.2690
512.322.8385 (Fax)

Version with Markings to Show Changes Made

IN THE CLAIMS:

Please cancel Claim 14, and amend Claims 1, 2, 8, 15-25, 35 and 40-42 as follows:

1. **(Twice Amended)** A computer system comprising:

a processor;

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive a **security code [verification data]**, the **security code [verification data]** confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the **security code [verification data]**;

an executable program code that verifies validity of the access token **by comparing the security code to a verification data on the access token, whereby if the security code matches verification data the access token is valid [using the verification data];**

an executable program code that receives a set of security policies from the access token in the processor **if the access token is valid [in response to the verification data]**; and

an executable program code that controls access to resources in the processor based on the security policies.

2. **(Twice Amended)** The computer system of claim 1 further comprising:

a nonvolatile storage device operably coupled to the processor;

a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the executable program code **verifying that the security code matches the verification data on the access token. [receiving valid verification data with the access token provided.]**

verification data on the access token. **[receiving valid verification data with the access token provided.]**

8. **(Twice Amended)** A computer system comprising:

a processor;

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive verification data, the verification data confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the verification data;

an executable program code that verifies validity of the access token using the verification data;

an executable program code that sets security policies in the processor; **[and]**

an executable program code that controls access to resources in the processor based on the security policies; and

a display device, wherein one of the one or more security policies includes one or more interface settings that control a desktop presentation on the display device.

Please cancel Claim 14 without prejudice or disclaimer.

15. **(Twice Amended)** **[The computer system of claim 14]** **A computer system comprising:**

one or more processors;

memory electrically interconnected to the one or more processors;

an operating system for controlling the operation of the one or more processors;

an access token communication device electrically interconnected to at least one of the one or more processors, the access token communication device being communicatively operable with an access token;

an input device electrically interconnected to at least one of the one or more processors, the input device operable to transmit a security code from a user to the one or more processors;

a nonvolatile storage device electrically interconnected to at least one of the one or more processors, the nonvolatile storage device including a nonvolatile memory;

a set of security policies associated with the operating system, the operating system operable to receive the security code for selectively enabling the set of security policies to limit access to the computer system; and

the operating system permitting access to the nonvolatile storage device and the one or more processors if the security code and the set of security policies match an authorization data stored in the nonvolatile memory,

wherein the access token further includes verification data, the verification data operable to provide the security policies to the nonvolatile memory if the security code matches an authentication code stored in the access token.

16. **(Twice Amended)** The computer system of claim **15** **[14]** wherein the operating system includes a BIOS and the BIOS is stored in the nonvolatile memory that is electrically interconnected to the one or more processors.

17. **(Amended)** The computer system of claim **15** **[14]** wherein the access token communication device includes a smart card communication device.

18. **(Amended)** The computer system of claim **15** **[14]** wherein the access token communication device includes network circuitry that is adapted to receive signals from one or more computers interconnected on a computer network.

Version with Markings to Show Changes Made

19. **(Amended)** The computer system of claim **15** **[14]** wherein the access token communication device includes a modem that receives signals from a communications line.

20. **(Amended)** The computer system of claim **15** **[14]** wherein the input device is a keyboard.

21. **(Amended)** The computer system of claim **15** **[14]** wherein the input device includes a biometric data reading device.

22. **(Amended)** The computer system of claim **21** **[14]** wherein the biometric data reading device includes a fingerprint scanner.

23. **(Amended)** The computer system of claim **21** **[14]** wherein the biometric data reading device includes a retinal scanning device.

24. **(Amended)** The computer system of claim **15** **[14]** wherein the nonvolatile storage device includes a hard disk drive.

25. **(Amended)** The computer system of claim **15** **[14]** further comprising a data access code stored in the nonvolatile memory, wherein a data request code corresponding to the data access code alters a state of the nonvolatile storage device.

35. **(Twice Amended)** A method of using an access token, said method comprising:

transferring one or more passwords from the access token to a computer system; **[and]**

receiving a user input password at the computer system; and

matching a computer system password with **[the combined user]** **the user input** password **with** the one or more passwords from the access token **to access the computer**

system, wherein the computer system password includes one or more security policies configured in the computer system.

40. **(Amended)** [An] **A communication device having an** access token for use with a computer system, said [access token] **communication device** comprising:

one or more security policies adapted to be used by **[a] the** computer system, wherein the one or more security policies are stored in an encrypted format; and

[an access] a security code stored on the access token, wherein the **communication device [access token]** transmits the one or more security policies in response to receiving **an authentication code [a data stream]** corresponding to the **[access] security** code.

41. **(Twice Amended)** A computer operable medium for protecting a computer system, said computer operable medium comprising:

means for reading an access token **containing a security policy for the computer system**;

means for receiving an authentication password **from a user**;

means for verifying the validity of the access token based on **a comparison of** the authentication password **to the security policy**;

means for setting security policies in the **[information handling] computer** system; and

means for unlocking a nonvolatile storage device on the **[information handling] computer** system.

42. **(Twice Amended)** An information handling system comprising:

means for reading an access token **containing a security policy for the information handling system**;

means for receiving an authentication password **from a user**;

means for verifying the validity of the access token based on **a comparison of** the authentication password **to the security policy**;

Version with Markings to Show Changes Made

means for setting security policies in the information handling system; and

means for unlocking a nonvolatile storage device on the information handling system.